International Journal of Research and Applications
Oct - Dec © 2014 Transactions; 1(4): 202-208
ISSN (online): 2349-0020
ISSN (print): 2394-4544

COMPUTERS | ORIGINAL ARTICLE

EFFICIENT MODEL AND MECHANISM FOR MULTIPARTY ACCESS CONTROL ON SOCIAL NETWORKS

S.RAVI[1] and A. Veera Swamy [2]
[1] M.Tech (pursuing) and [2] Assistant Professor
[12]Dept of CSE, Universal college of engineering and Technology, Guntur, A.P.
[1] sikharavi@gmail.com and [2] cseucet1122@gmail.com.

ABSTRACT

Online social networks (OSNs) have experienced tremendous growth in recent years and become a de facto portal for hundreds of millions of Internet users. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. To this end, we propose an approach to enable the protection of shared data associated with multiple users in OSNs. We formulate an access control model to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Besides, we present a logical representation of our access control model which allows us to leverage the features of existing logic solvers to perform various analysis tasks on our model. We also discuss a proof-of-concept prototype of our approach as part of an application in facebook and provide usability study and system evaluation of our method.

Keywords: Multi party, Leverage, prototype, access control, protection.

1. INTRODUCTION

ONLINE social networks (OSNs) such as Twitter, Face book, and Google+ are genetically described to enable people to share personal and public information and make social Connections with friends, coworkers, colleagues, family, and even with newcomer. In recent years, we have seen unique growth in the application of OSNs. For example Face book, one of model social network sites, Application that it has more than 800 million active users and over 30 billion pieces of fulfilled(web links, news stories, blog posts, notes, photo albums, and so on.) shared each month [3]. To care for user data, access control has become an essential feature of OSNs [2], [4].

An exemplary OSN provides each user with an essential space containing profile information, a list of the user's friends, and webpage's, such as wall in Face book, where users and friends can post content and leave messages. A user profile generally has information with respect to the user's education, birthday, gender, interests, and contact information, and work history. In addition, users can not only upload content into their own or others' spaces but also tag other users who come out in the content. Each tag is a

clear reference that links to a user's space. For the safety of user data, current OSNs indirectly require users to be system and policy administrators for handle their data, where users can reduce data sharing to a particular set of honorable users. OSNs generally use user relationship and group membership to categorize between trusted and entrusted users. For example, in Face book, users can grant friends, friends of friends (FOF), groups, or public to access their data, depending on their personal approval and privacy requirements.

Although OSNs presently implement simple access regulation mechanisms grant users to control access to information consist of in their own spaces, users, unfortunately, have no control over information residing outside their spaces. For instance, if a user posts a comment in a friend's space, she/he cannot define which users can look the comment. In another case, when a user uploads a photo and tags to friends who occur the photo, the tagged friends cannot possible restrict who can see this photo, even though the tagged friends may include particular privacy interest about the photo. To address such a critical problem, exploratory security structure has been provide by actual OSNs. For example, face book grant the tagged users to remove the tags associated to their profiles or report these violations querying Face book managers to remove the details that they do not want interest to share with the public. However these uncomplicated protection mechanisms suffer from certain conditions. On one hand removing a tag from a photo can only block, other members seeing to remove the tags linked to their profiles or report violations asking Facebook managers to remove the contents that they do not want to share with the public. However, these simple protection mechanisms suffer from several limitations. On one hand, removing a tag from a photo can only prevent other members from seeing a user's profile by means of the association link, but the user's image is still contained in the photo. Since original access control policies cannot be changed, the user's image continues to be revealed to all authorized users. On the other hand, reporting to OSNs only allows us to either keep or delete the content. Such a binary decision from OSN managers is either too loose or too restrictive, Relying on the OSN's administration and requiring several people to report their request on the same content. Hence, it is essential to develop an effective and flexible access control mechanism for OSNs, accommodating the special authorization requirements coming from multiple associated users for managing the shared data collaboratively.

2. EXISTING SYSTEM

The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs. The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work provided a solution for collective privacy management in OSNs. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content.

A user profile usually includes information with respect to the user's birthday, gender, interests, education and work history, and contact information. In addition, users can not only upload content into their own or others' spaces but also *tag* other users who appear in the content. Each tag is an explicit reference that links to a user's space. For the protection of user data, current OSNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. OSNs often use user relationship and group membership to distinguish between trusted and untrusted users. For example, in Facebook, users can allow friends, friends *of* or public to access their data,

depending on their personal authorization and privacy requirements.

3. PROPOSED SYSTEM

In Proposed System we implemented a proof-of-concept Facebook application for the collaborative management of shared data, called *MController.* Our prototype application enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item. It is worth noting that our current implementation was restricted to handle photo sharing in OSNs. Obversely, our approach can be generalized to deal with other kinds of data sharing and comments, in OSNs as long as the stakeholder of shared data are identified with effective methods like tagging or searching. The proposed system shows a novel solution for collaborative management of shared data in OSNs. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model. A proof-of-concept implementation of our solution called *MController* has been discussed as well, followed by the usability study and system evaluation of our method. Indeed, a flexible access control mechanism in a multi-user environment like OSNs should allow multiple controllers, who are associated with the shared data, to specify access control policies. As we identified previously in the sharing patterns in addition to the *owner* of data, other controllers, including the *contributor*, *stakeholder* and *disseminator* of data, need to regulate the access of the shared data as well. In our multiparty access control system, a group of users could collude with one another so as to manipulate the final access control decision.

3.1 MULTIPARTY ACCESS CONTROL MODEL FOR OSNS

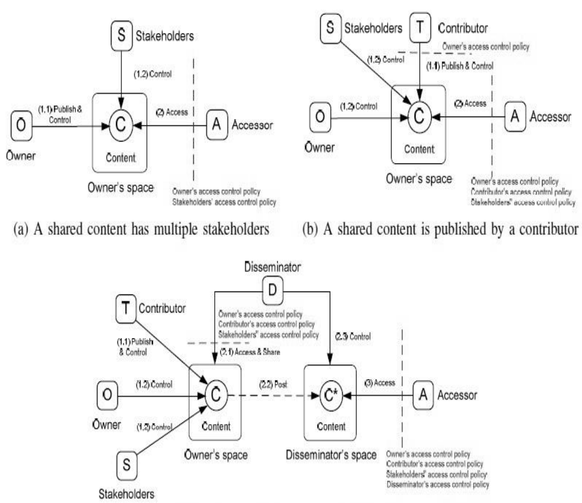
In this section, we formulated a MPAC model for OSNs, as well as a policy based evaluation scheme and a policy mechanism for the enforcement and specification of MPAC policies in OSNs.

3.1.1 MPAC Model

An OSN can be represented by a relationship network, a set of user groups and a collection of user data. The relationship network of an OSN is a directed labeled graph, where each node denotes a user and each edge represents a relationship between two users. The label associated with each edge indicates the type of the relationship. Edge direction denotes that the initial node of an edge establishes the relationship and the terminal node of the edge accepts the relationship. The number and type of supported relationships rely on the specific OSNs and its purposes. Besides, OSNs include an important feature that allows users to be organized in groups (or called circles in Google+), where each group has a unique name. This feature enables users of an OSN to easily find other users with whom they might share specific interests (e.g., same hobbies), demographic groups (e.g., studying at the same schools), political orientation, and so on. Users can join in groups without any approval from other group members. Furthermore, OSNs provide each member a Web space where users can store and manage their personal data including profile information, friend list and content. Recently, several access control schemes have been proposed to support fine-grained authorization specifications for OSNs. Unfortunately, these schemes can only allow a single controller, the resource owner, to specify access control policies. Indeed, a flexible access control mechanism in a multi-user environment like OSNs should allow multiple controllers, who are associated with the shared data, to specify access control policies.

Profile sharing: An appealing feature of some OSNs is to support *social applications* written by

third-party developers to create additional functionalities built on the top of users' profile for OSNs [1], [5]. To provide meaningful and attractive services, these social applications consume user profile attributes, such as name, birthday, activities, interests, and so on. To make matters more complicated, social applications on current OSN platforms can also consume the profile attributes of a user's friends. In this case, users can select particular pieces of profile attributes they are willing to share with the applications when their friends use the applications. At the same time, the users who are using the applications may also want to control what information of their friends is available to the applications since it is possible for the applications to infer their private profile attributes through their friends' profile attributes [30], [38]. This means that when an application accesses the profile attributes of a user's friend, both the user and her friend want to gain control over the profile attributes.



(a) A shared content has multiple stakeholders (b) A shared content is published by a contributor

(c) A disseminator shares other's content published by a contributor.

Relationship sharing: Another feature of OSNs is that users can share their relationships with other members. Relationships are inherently bidirectional and carry potentially sensitive information that associated users may not want to disclose. Most OSNs provide mechanisms that users can regulate the display of their friend lists. A user, however, can only control one direction of a relationship. Let us consider, for example, a scenario where a user Alice specifies a policy to hide her friend list from the public. However, Bob, one of Alice's friends, specifies a weaker policy that permits his friend list visible to anyone. In this case, if OSNs can solely enforce one party's policy, the relationship between Alice and Bob can still be learned through Bob's friend list. Figure 1(b) shows a relationship sharing pattern where a user called *owner*, who has a relationship with another user called *stakeholder*, shares the relationship with an *accessor*. In this scenario, authorization requirements from both the owner and the stakeholder should be considered. Otherwise, the stakeholder's privacy concern may be violated.

Content sharing: OSNs provide built-in mechanisms enabling users to communicate and share contents with other members. OSN users can post statuses and notes, upload photos and videos in their own spaces, tag others to their contents, and share the contents with their friends. On the other hand, users can also post contents in their friends' spaces. The shared contents may be connected with multiple users. Consider an example where a photograph contains three users, Alice, Bob and Carol. If Alice uploads it to her own space and tags both Bob and Carol in the photo, we call Alice the *owner* of the photo, and Bob and Carol *stakeholders* of the photo. All of them may specify access control policies to control over who can see this photo.

3.2 MULTIPARTY POLICY EVALUATION

Two steps are performed to evaluate an access request over multiparty access control policies. The first step checks the access request against the policy specified by each controller and yields a decision for the controller. The *accessor* element in a policy decides whether the policy is applicable to a request. If the user who sends the request belongs to the user set derived from the *accessor* of a policy, the policy is applicable and the evaluation process returns a response with

the decision (either permit or deny) indicated by the *effect* element in the policy. Otherwise, the response yields deny decision if the policy is not applicable to the request. In the second step, decisions from all controllers responding to the access request are aggregated to make a final decision for the access request.

4. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a Working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. In Owner module let *d* be a data item in the space m of a user *u* in the social network. The user *u* is called the owner of *d*

Fig 1: Signup for social network

The user *u* is called the contributor of *d*. We specifically analyze three scenarios—profile sharing, relationship sharing and content sharing—to understand the risks posted by the lack of collaborative control in OSNs. In this the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes. Thus, it enables the owner to discover potential malicious activities in collaborative control. The detection of collusion behaviors in collaborative systems has been addressed by the recent work.In Contributor module let *d* be a data item published by a user *u* in someone else's space in the social network. The contributor publishes content to other's space and the content may also have multiple stakeholders (e.g., tagged users). The memory space for the user will be allotted according to user request for content sharing. A shared content is published by a contributor.

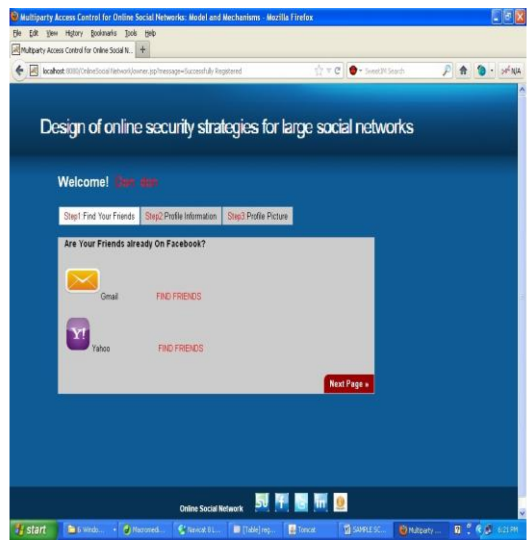


Fig 2: various social networking sites, those provides free space

In Stakeholder module let *d* be a data item in the space of a user in the social network. Let *T* be the set of tagged users associated with *d*. A user *u* is called a stakeholder of *d*, if *u* 2 *T* who has a relationship with another user called stakeholder, shares the relationship with an *accessor*. In this scenario, authorization requirements from both the owner and the stakeholder should be considered. Otherwise, the stakeholder's privacy concern may be violated. A shared content has multiple stakeholders.

In Disseminator module let *d* be a data item shared by a user *u* from someone else's space to his/her space in the social network. The user *u* is called a disseminator of *d*. A content sharing pattern where the sharing starts with an originator (owner or contributor who uploads the content) publishing the content, and then a disseminator views and shares the content. All access control policies defined by associated users should be enforced to regulate access of the content in disseminator's space. For a more complicated case, the disseminated content may be further re-

Fig 3: Setting friends list to view the shared item

disseminated by disseminator's friends, where effective access control mechanisms should be applied in each procedure to regulate sharing behaviors. Especially, regardless of how many steps the content has been re-disseminated, the original access control policies should be always enforced to protect further dissemination of the content.MPAC is used to prove if our proposed access control model is valid. To enable a collaborative authorization management of data sharing in OSNs, it is essential for multiparty access control policies to be in place to regulate access over shared data, representing authorization requirements from multiple associated users. Our policy specification scheme is built upon the proposed MPAC model.

Accessor Specification: Accessors are a set of users who are granted to access the shared data. Accessors can be represented with a set of user names, asset of elationship names or a set of group names in OSNs.

5. CONCLUSION

Multiparty access control for online social network has proposed a novel solution for collaborative management of shared data in OSNs. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model. A proof-of-concept implementation of our solution called *MController* has been discussed as well, followed by the usability study and system evaluation of our method. As part of future work, we are planning to investigate more comprehensive privacy conflict resolution approach and analysis services for collaborative management of shared data in OSNs. Also, we would explore more criteria to evaluate the features of our proposed MPAC model. For example, one of our recent work has evaluated the effectiveness of MPAC conflict resolution approach based on the

tradeoff of privacy risk and sharing loss. In addition, users may be involved in the control of a larger number of shared photos and the configurations of the privacy preferences may become time-consuming and tedious tasks. Therefore, we would study inference-based techniques for automatically configure privacy preferences in MPAC. Besides, we plan to systematically integrate the notion of trust and reputation into our MPAC model and investigate a comprehensive solution to cope with collusion attacks for providing a robust MPAC servce in OSNs.

6. REFERENCES:

[1]Face book Developers. http://developers.facebook.com/.

[2] Face book Privacy Policy. http://www.facebook.com/policy.php/.

[3] Face book Statistics. http://www.facebook.com/press/info.php?.

[4] Google+ Privacy Policy. http://http://www.google.com/intl/en/+/policy/.

[5] Open Social Framework. http://code.google.com/p/opensocial-resources/.

[6] The Google+ Project. https://plus.google.com.

[7] A. Besmer and H. Richter Lipford. Moving beyond untagging: Photoprivacy in a tagged world. In Proceedings of the 28th international conference on Human factors in computing systems, pages 1563–1572. ACM, 2010.

8] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belonging to us: automated identity theft attacks on social networks. In Proceedings of the 18th international conference on World wide web, pages 551–560. ACM, 2009.

[9] B. Carminati and E. Ferrari. Collaborative access control in online social networks. In Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Work sharing (Collaborate Com), pages 231–240. IEEE, 2011.

[10] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, pages 1734–1744. Springer, 2006.